CLAIMS:

1. (Currently Amended) A method of synchronizing encryption in a communications network between a transmitting set and a receiving set, the method comprising the steps of:

   (a) creating, at the transmitting set, a bitstream, said bitstream including a synchronization vector derived from a session key;

   (b) generating, at the transmitting set, an encryption signal based upon said session key and encrypting said bitstream with said encryption signal;

   (c) transmitting said encrypted bitstream from the transmitting set to the receiving set; ~~and~~

   (d) generating, at the receiving set, said encryption signal based upon said session key and decrypting said encrypted bitstream using said encryption signal to identify said synchronization vector~~,~~; and

   (e) synchronizing said encryption signal to said encrypted bitstream based on identification of said synchronization vector to permit recovery of said bitstream from said encrypted bitstream.

   ~~whereby said synchronization vector is used to synchronize the encryption and decryption of data~~.

2. (Original) The method claimed in claim 1, wherein said synchronization vector comprises said session key.

3. (Original) The method claimed in claim 2, wherein said step of decrypting includes applying a feedback cipher to said encrypted bitstream to obtain a decrypted output, and comparing said decrypted output with said session key.

4. (Original) The method claimed in claim 1, wherein said bitstream includes random bits followed by said synchronization vector, followed by voice data.

5. (Original) The method claimed in claim 1, including a first step of calculating said session key from a common seed value.

6. (Original) The method claimed in claim 5, wherein said step of calculating said session key includes applying a first function to said common seed value to generate said session key.

7. (Original) The method claimed in claim 6, further including a step of applying a second function to said session key to produce a new seed value for use in subsequent communications.

8. (Currently Amended) A system for the secure transmission of information over a communications network, the system comprising:

(a) a transmitting set, said transmitting set having an encryption module, wherein said encryption module receives a session key, generates an encryption signal based upon said session key, generates a bitstream, said bitstream including a synchronization vector derived from said session key, and encrypts said bitstream with said encryption signal to transmit an encrypted bitstream; and

(b) a receiving set, said receiving set including a decryption module, wherein said decryption module receives said encrypted bitstream from said transmitting set, generates said encryption signal based upon said session key, and decrypts said encrypted bitstream using said encryption signal to identify said synchronization vector,

wherein said decryption module is configured to synchronize said encryption signal to said encrypted bitstream based on identification of said synchronization vector to permit recovery of said bitstream from said encrypted bitstream ~~whereby said synchronization vector is used to synchronize the encryption and decryption of data~~.

9. (Original) The system claimed in claim 8, wherein said synchronization vector

comprises said session key.

10. (Original) The system claimed in claim 9, wherein said decryption module includes a feedback cipher and a comparator, wherein said feedback cipher produces a decrypted output, and wherein said comparator compares said decrypted output with said session key so as to identify said synchronization vector.

11. (Original) The system claimed in claim 8, wherein said bitstream includes random bits followed by said synchronization vector, followed by voice data.

12. (Original) The system claimed in claim 8, wherein said transmitting set includes a common seed value and a cryptographic engine for calculating said session key from said common seed value.

13. (Original) The system claimed in claim 12, wherein said cryptographic engine includes a first function for converting said seed value into said session key.

14. (Original) The system claimed in claim 12, wherein said cryptographic engine includes a second function for converting said session key into a new common seed value.

15. (Currently Amended) A handset for use in a communications network for secure communications between the handset and a corresponding set, the handset comprising:

an encryption module, said encryption module receiving a session key, generating an encryption signal based upon said session key, generating an output bitstream, said output bitstream including a synchronization vector derived from said session key, and encrypting said output bitstream with said encryption signal to transmit an encrypted bitstream; and

a decryption module, said decryption module receiving said session key, generating said encryption signal based upon said session key, receiving an incoming bitstream from the corresponding set, and decrypting said

incoming bitstream using said encryption signal to identify said synchronization vector,

wherein said decryption module is configured to synchronize said encryption signal to said encrypted bitstream based on identification of said synchronization vector to permit recovery of said bitstream from said encrypted bitstream~~whereby said synchronization vector is used to synchronize the encryption and decryption of data.~~

16. (Original) The handset claimed in claim 15, wherein said synchronization vector comprises said session key.

17. (Original) The handset claimed in claim 16, wherein said decryption module includes a feedback cipher and a comparator, wherein said feedback cipher produces a decrypted output, and wherein said comparator compares said decrypted output with said session key so as to identify said synchronization vector.

18. (Original) The handset claimed in claim 15, wherein said output bitstream includes random bits followed by said synchronization vector, followed by voice data.

19. (Original) The handset claimed in claim 15, further including a common seed value and a cryptographic engine for calculating said session key from said common seed value.

20. (Original) The handset claimed in claim 19, wherein said cryptographic engine includes a first function for converting said seed value into said session key.

21. (Original) The handset claimed in claim 19, wherein said cryptographic engine includes a second function for converting said session key into a new common seed value.

22. (Original) A method for secure transmission of streamed voice data in a network between a transmitting set and a receiving set, the method

comprising the steps of:

(a) providing the transmitting set and the receiving set with a seed value and a predetermined first function;

(b) at each of the transmitting set and the receiving set, applying the predetermined first function to the seed value to produce a session key;

(c) at the transmitting set, generating an encryption signal based upon said session key and encoding the streamed voice data with said encryption signal to produce an encrypted bitstream;

(d) transmitting said encrypted bitstream from the transmitting set to the receiving set; and

(e) at the receiving set, generating said encryption signal based upon said session key and decoding said encrypted bitstream using said encryption signal to obtain the streamed voice data.

23. (Original) The method claimed in claim 22, wherein said step of providing includes distributing said seed value to the transmitting set and the receiving set by a call server via the network.

24. (Original) The method claimed in claim 22, further including a step of receiving an index from a call server, and wherein said step of applying the predetermined first function includes repeating application based upon said index.

25. (Original) The method claimed in claim 22, further including a step of applying a second function to said session key to produce a new seed value.

26. (Original) The method claimed in claim 22, wherein said step of encoding the voice data includes the steps of generating a bitstream, wherein said bitstream includes a synchronization vector and the voice data, said synchronization vector comprising said session key, and encrypting said

bitstream with said encryption signal to produce an encrypted bitstream.

27. (Original) The method claimed in claim 26, wherein said step of decoding said encrypted bitstream includes the steps of decrypting said encrypted bitstream to produce a decrypted bitstream and comparing said decypted bitstream with said session key to identify said synchronization vector.

28. (Original) A system for secure transmission of streamed voice data in a network, the system comprising:

(a) a transmitting set, the transmitting set including an encoder, said encoder having a first cryptographic engine and an encrypter, said first cyptographic engine including a first function and generating a session key from applying said first function to a seed value, said first cryptographic engine further generating an encryption signal based upon said session key, said encrypter receiving the streamed voice data and the encryption signal and producing an encrypted bitstream; and

(b) a receiving set, the receiving set including a decoder, said decoder having a second cryptographic engine and a decrypter, said second cyptographic engine including said first function and generating said session key from applying said first function to said seed value, said cryptographic engine further generating said encryption signal based upon said session key, said decrypter receiving said encrypted bitstream and said encryption signal and producing the streamed voice data.

29. (Original) The system claimed in claim 28, further including a call server for distributing said seed value to the transmitting set and the receiving set via the network.

30. (Original) The system claimed in claim 28, wherein said first and second cryptographic engines each include a second function for converting said session key to a new seed value.

31. (Original) The system claimed in claim 28, wherein said encoder includes a vocoder for generating a bitstream, said bitstream including a synchronization vector and the streamed voice data, said synchronization vector being said session key, and wherein said encrypter encrypts said bitstream to produce said encypted bitstream.

32. (Original) The system claimed in claim 31, wherein said decoder includes a comparator, said comparator receiving said decrypted bitstream and said session key and outputting a sync signal in response to a match between said decrypted bitstream and said session key.

33. (Original) The system claimed in claim 28, wherein said encrypter includes an XOR operator.

34. (Original) The system claimed in claim 33, wherein said decrypter includes an XOR operator.